IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 4, August 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Emerging Issues in Cyber Security for Institutions of Higher Education

[1] Mayieka Jared Maranga; [2] Dr. Masese Nelson

[1, 2] Department of Computer Science and IT,
Kabarak University - Kenya

Abstract - Institutions of higher learning find themselves engaged in an expensive defense race in buying current security tools and changing their strategies in countering latest cyber security attacks. These strategies are meant to promote operational protection and response to potential attacks on their cyberspace. In the meantime, the attackers are continuously finding ways around those set tools and are able to switch their strategies to hit their different targets. This paper therefore looks at ways through which these organizations are attacked, the extent of the attacks and how the institutions of higher learning can prepare and defend themselves against cyber-attacks. Systematic Literature Review was used to dig deeper to the existing secondary data. It was indeed discovered that Institutions of higher learning are frequently attacked and infiltrated for reasons such as modification of data such as school fees etc. by both internal agents such as students and staff and external agents such as competitors and malicious attackers. We finally make recommendations on what such institutions should do to defend themselves against such attacks.

Keywords - *cyber security, cybercrime, cyber ethics, social media, & cloud computing*

1. Introduction

Nowadays people are able to send and receive data online in any form including e-mails, audio files, and video files, etc. just by a click of a button. A question to ask ourselves is, do we ever stop to think how secure our data is being conveyed to our recipient without any leakage? The answer to this question can only be found in in cyber security. Currently Internet is growing rapidly among all other infrastructure in everyday life. Numerous technologies are changing the face of the world and how we do things. Due to these rapidly emerging technologies, many organizations are unable to protect their private information and resources in an absolute & effective manner hence facilitating cybercrimes day by day (Harold & Micki, 2003).

Currently, over 60 per cent of the entire commercial transactions are completed online. So, this arena requires a high eminence of security for transparent and unsurpassed transactions (Cheng, 2016). Many institutions of higher learning are massively engaging in building their Cyberspaces in a bid to advance their service delivery to their highest level best almost all the time. Cyber Security therefore becomes very critical especially because it plays a central role in information technology, service delivery and meeting the ever increasing and overrated customer expectations (Resources Management, 2018). The process of securing organizational data, their information, infrastructure and other internal resources such as trade secrets, and copyrights etc. which largely depend on the deployed technology is becoming one of the biggest challenges to many organizations. This has complicated people's imaginations to an extent that whenever there is a thought about cyberspace and cyber security, one thing comes to people's mind is, 'cybercrime'. Various institutions including governments and other private sector corporations are taking numerous measures to could potentially thwart these crimes (Mostafa, Mohamed, & Faddoul, 2017). Above and beyond the various measures, cyber security remains a huge concern to many companies and governments.

1.1. Problem Statement

The significance and impact of the cyberspace and the internet in general to the academic and professional development of students, staff and faculty of institutions of higher learning cannot be underestimated. However, this contribution has been blemished and stained by the continuous development of emerging ways of cybercrime. The cyberspace has similarly become an atmosphere where serious and expensive cybercrime thrives. Every passing day, we hear of more and more disturbing cases of cybercrime being perpetrated on different institutions and more specifically, on institutions of higher learning (Folashade & Adeta, 2013).

1.2. Emerging issues in institutions of higher learning

In the Kenyan context for instance, the Public Sector ICT Survey Report 2016 on cybercrime confirm that cyber-attacks are launched comparatively more in institutions of higher learning compared to other public sector organizations as shown in figure 1 below. These attacks are characterized as data exfiltration, cyber stalking, data interception, identity theft, Denial of service attack, network interference, data theft and cybercrime related to data/information access such as unauthorised and unauthenticated data/information access, virus distribution among others. Due to these attacks, institutions of higher learning have to incur huge economical and service delivery mislay. Most of these institutions have testified against various cases of confidential data/information loss, modification of certain data/information such as alteration on student‘s school fee balances and modification of student grades among other breaches (Communications Authority of Kenya; Kenya National Bureau of Statistics, 2017).

Other challenged such as cyber espionage is common especially when institutions what to understand why other institutions seem to be successful than others and when some competing institutions want to get hold of the academic curriculums of the competitor including the copyrighted trade secrets.

Student hactivism is also on the rise. A report by Cyberoam (2016) placed Kenya among African countries leading in cyber-attacks, after Egypt, Morocco and South Africa. The university “hacktivists” interfere with school information systems with an aim of adjusting student grades and their school fee balances (Business Daily, 2015).

> *“Hacking has become a booming business in schools, especially towards the end of semesters and during the graduation time. Cyber security in institutions of higher learning is therefore one of the areas that require a deep look with proper solutions developed, including identifying the minimum level of security for any learning institution,”* said the Cyberoam manager Philip Obondy.

With such ugly happening, it is apparent that institutions of higher learning are suffering a lot of impediments in their pursuit for academic excellence.

The above situation therefore confirms the necessity to conduct a research on cyber security on what challenges the institutions of higher learning are facing and how to protect how students, faculty and staff interact, collaborate, and conduct business in the Cyberspace.

1.3. Objective of the Paper

This paper mainly focuses on emerging issues in cyber security for institutions of higher learning and proposing remedies and ethics necessary in changing the face of cyber security in such institutions.

2. Related Literature

2.1. Cyber Crime in Institutions of Higher Learning

Cybercrime referrers to any illegal activity involved in by using a computer or any electronic devises as its primary means of commission and theft. Many governments in the world have extended this definition to cover their jurisdictions. For instance, the United States of America expanded this definition of cybercrime to include any unlawful activity that uses a computer for the storage of evidence. In Kenya, the Kenya Information and Communications Act (2013) defines cybercrime as “a criminal activity in which computers or computer networks are a tool, a target or place of criminal activity and include everything from electronic cracking to denial of service attacks. Cybercrime also includes traditional crimes in which computers or networks are used to enable illicit activity.”

Institutions of higher learning’s Chief Information Security Officers (CISOs) especially in developing nations are contending with a diversity of issues as they attempt to preserve their campuses from cybercriminals (Trend, 2015). They are not alone. In reality, the number one problem for higher education institutions’ Information Technology cream of the crop recently is information security, according to (Tanya R. , 2015), at EDUCAUSE, a non-profit association of Information Technology leaders in higher education in the United States. Information security frequently shows up on the EDUCAUSE’s Top 10 list, though it earned the first spot in 2016.

> *"I think information security rose to the top of the list in 2016 because institutional leadership is becoming more aware of the risks that arise when evolving technologies, business practices and user expectations collide in a way that doesn’t protect institutional resources, institutional data, or user data that institutions have been entrusted to protect,"* said Joanna Grama, director of the IT

Governance, Risk and Compliance Program and cybersecurity programs at EDUCAUSE.

The Chief Information Security Officers for Institutions of higher education have to make selections around what cyber security risks they will deal with first and which ones among many will drop to the lowest of the significance list. Many times, the CISOs don't get to the low significance items, which is the reason so many Institutions of higher education are attacked in the recent past.

The following are the eight major challenges cited by many CISOs for Institutions of higher education that they are dealing with on a daily basis.

i. Phishing

Phishing is a social engineering attack frequently used to steal user data, including login identifications. It occurs when an attacker, camouflages as a trusted entity then dupes a victim into opening an email, instant message, or text message (Christopher & Michele, 2015). Students and other university users open emails that are designed to trick them into clicking a malicious link thereby ending up downloading malicious software attachments. These attachments will either infect their computers or the whole network, or are likely inadvertently give their access rights to the attackers. Take for instance, if a lecturer is duped and his credentials given to the cybercriminal, the attacker is likely to do many things with the acquired credentials including changing of students' grades, either for fun or at a pay by the students, can alter the attendance of the students, etc.

Therefore, educating faculty, students and staff of institutions of higher learning on the ways of avoiding phishing, will go a long way to helping secure institutional cyberspaces.

a) Deceptive Phishing

This is any attack by which impostors mimic a legitimate corporation and try to steal people's personal information or login credentials. The emails that they use frequently use intimidations and a sense of urgency to scare user into undertaking the attackers' request. For instance, PayPal scammers can send out an attack email that instructs users to click on a link in order to correct an inconsistency with their account. In reality, the link redirects the user to a bogus PayPal login page that gathers a user's login credentials and sends them to the attackers (David B. , 2016). Most universities are targeted in this way especially because there is a feeling that students are able to be convinced easily.

The accomplishment of deceptive phishing lies on how closely the attack email looks like a legitimate organization's official communication. As a consequence, users should examine all URLs prudently to understand if they are redirected to an unidentified website. They should also look out for generic greetings, grammar errors, and spelling mistakes dispersed throughout the email.

b) Spear Phishing

The goal of spear phishing is the same as that of deceptive phishing i.e. to lure the target into clicking on a malicious URL or email attachment, to give their personal data. For example, impostors customize their attack emails with the victim's name, position, organization; office phone numbers etc. in an attempt to trick the victim into believe that they have a connection with the sender of the message. This type of phishing is particularly common on social media sites such as LinkedIn, where the aggressors can use multiple sources of data to craft a targeted attack email. Most students are common in social media sites hence making it possible to such attacks to be common in institutions of higher learning.

To defend oneself against this type of an attack, institutions should carry out continuous employee security awareness trainings which among other things, discourage users from dissemination of sensitive personal or company information on their social media sites (David B. , 2016). The institutions of higher learning should also capitalize in solutions that are proficient in the analysis of the incoming emails from known malicious links/email attachments.

c) Pharming

This is a technique of attack that stem from domain name system (DNS) cache poisoning. As users become more knowledgeable to traditional phishing methods, some hoaxers are forsaking the idea of "enticing" their victims entirely. Instead, they are resorting to pharming. The Internet's naming system uses DNS servers to translate alphabetical website names, such as "www.aiu.ac.ke," to arithmetical IP addresses that are used for locating computer services and devices on the internet. Under a DNS cache, a pharmer targets a DNS server and changes an IP address allied with an alphabetical website name to their different website. That means a hacker can redirect victims to a malicious site of their choice even if the victims keyed in the exact website name.

To protect users against pharming attacks, Institutions of higher learning should encourage students and staff to key in login credentials only on HTTPS-protected sites. They should also install anti-virus software on all organizational devices and install virus database updates/patches, along with security upgrades distributed by a trusted Internet Service Provider (ISP), on a regular basis.

d) Google Docs Phishing

This is a type of phishing where the attackers target Google Drive. Explicitly, as Google Drive supports documents, spreadsheets, presentations, photos and even an entire website, these kinds of phishers target to abuse the service by creating web pages which closely mimic the Google account log-in screen to harvest user credentials (David B. , 2016). In July of 2015 for instance, a group of attackers did just that and not only did Google innocently host that bogus login page, but a Google SSL certificate also protected the page with a secure connection.

Therefore, the institutions should encourage the students and staff to employ 2SV to protect them against this type of attack. Students can enable the security feature via either SMS messaging or the Google Authenticator app.

e) CEO Fraud

This type of phishing involves an attempt by the attackers to harpoon an organization's executive and steal their login credentials. In the event their attacks succeed, they then choose to conduct CEO fraud which is the second phase of an official executive email address compromise scam where the cybercriminals impersonate the organization's CEO and misuse that individual's email address to authorize deceitful wire transfers and transactions to a financial institution(s) of their choice (David B. , 2016). This is a typical whaling attack which usually works because the executives often don't participate in security awareness training with their juniors (Tanya R. , 2015).

Institutions of higher learning are likely to lose their finances to such deceitful attacks. Equally, such tricks are likely to dupe members of staff to release information that is otherwise privileged and top secret to the management of the said institutions. To counter these kinds of threat, as well as the risk of CEO fraud, all company personnel including executive officials, students and faculty should undergo continuous security awareness training. Institutions of higher learning can also consider amending their financial policies so that no one can authorize a financial transaction via email.

2.2. User Education

User education in the context of cyber security is a security awareness training which is an official process of educating institutional users about computer security and the associated risks. A good security awareness package in an institution of higher learning is meant to educate faculty, students and staff about institutional policies and procedures for working with information technology and the best practices that will ensure safe and secure institutional cyberspace.

Students in most of the institutions of higher learning usually have a full school work load, the faculty and staffs are also working almost all the time etc. With such busy timetables, cybersecurity awareness habitually takes a backseat to teaching and learning (Tanya R. , 2016). This means therefore that there is no proper training, sufficient enough to enable the users, Students and staff, to be fully equipped to counter computer insecurity (Trend, 2015).

> According to Jakob Nielsen (2004), "*Internet scams cannot be thwarted by placing the burden on users to defend themselves at all times. Stressed users need protection, and the technology must change to provide this.*"

According Jakob (2004) User education should not be the main approach to countering security problems for three reasons.

a. First, and most outstandingly, **it doesn't work**. Computer security is too complicated and so, it is simply unrealistic to assume that average users can keep up with them. It is possible to tell people not to click on attachments in emails from unfamiliar persons, but then what will happen when the attackers send email that ostensibly comes from your boss, your wife, or your best friends? In a contemporary workplace, one cannot do his/her work short of clicking on attachments.
b. Second, user education **places the burden on the wrong bearers**. It's like the old Wild West, where the reaction to crime was that all men carried guns. In enlightened society, we've abandoned this approach in favour of a specialised law enforcement agency to deal with offenders. When there is a divergence between technology and users, the answer should not be to change people. The answer should be to change the technology. Technology and the Internet were established under with a presumption that everyone is truthful and there would never be any

crime. That's clearly no longer true, and we need to rearchitect the technology accordingly.

c. Third, the more we keep the burden on users as opposed to fixing the technology, we'll **never realize the technology's and cyber** space's **full paybacks**. In its place, we'll alarm users and make them be more unwilling to use technology to its full potential.

Generally, user education is also an important part of sociological development. The threats we face on the cyber space are not novel in notion: only in technological application. Social engineering attacks have been in existence for so long but the economy of scale in the execution of such attacks was comparatively minor that extensive education in recognition of these techniques was not deemed essential (David H. , 2017). The Internet has resulted in a rapid upsurge in the use of social engineering attacks to where knowledge of how these attacks are perpetrated is a required life skill in modern society. Institutions of higher learning therefore need to shift a lot of their emphasis from blaming user education to more technological solutions (Ashwin, 2016).

2.3. Security Technology Planning for the Next-Generation

This is one of the most expensive races for institutions of higher learning. The next generation of enterprise IT comprises heart-rending past transactional systems to a multifaceted interrelated bionetwork that advances the mission and goals of the organization. Developing an operative technology policy necessitates a profound understanding of institutional culture and needs than ever before, as well as a sharper emphasis on data integration and data governance (EDUCAUSE). This complicates cyber security of such institutions. It is difficult for these institutions to pull alongside the tools that the cybersecurity industry produces based on the limited financial resources that they have. Institutions of higher learning, especially in developing countries are limited by resources and in Kenya, a number of the universities are shrinking and almost closing down (Tanya R. , 2016). That said, these institutions must work out a plan for how they will make certain that their security tools are as up to date as probable.

2.4. Failure to make High-Profile Information Security Strategy

For a long time, cyber security has not been topping the list of leaders of institutions of higher learning's priorities (Tanya R. , 2016). Currently however, with dangers and consequences increasing, it's imperative to get security on the radar of the company's executive level and begin an all-inclusive strategy that has buy-in from the top down.

2.5. Cloud Security

Most universities are running away from buying some servers and software and so opting for Cloud computing. This service works well for the Information Technology side of the university, but it also presents challenges for CISOs. Matt Morton, CISO and assistant CIO at the University of Nebraska at Omaha, (Tanya R. , 2016) said

> *"The cloud has taken off like crazy, and it's a great help, but at the same time, it's complicated from an information security perspective because there's a lot of due diligence that has to take place".*

2.6. Business Intelligence and Analytics

Institutions of Higher education are under rising pressure to upsurge student graduation and perseverance rates. Several funders to these institutions in various countries base their funding on how these institutions they're doing on these kinds of outcomes. Business intelligence and analytics therefore express a lot potential to help these institutions break down their data silos then use the statistics they have to make a transformation. Business intelligence is about investigating the data to understand what's going on across the institution and then acting on that report. Gordon Wishon, (Tanya R. , 2015), CIO of Arizona State University, stated that:

> *"Too often our data has grown up in silos with different departments feeling that they own the data. We consider data to be an institutional asset, and we're taking an enterprise view of data and how it should be collected and maintained and ultimately used."*

Whereas business analytics characteristically gets more investment from such institutions than learning analytics, both types can match each other. Eden Dahlstrom, director of research at EDUCAUSE (Tanya R. , 2015), said:

> *"There are overlapping interests between the business and institutional analytics and the learning analytics, and I think that's going to be the sweet spot,"*

2.7. Unsecure Personal Devices

The tendency of students and faculty members bringing their own devices to the institutions compounds presents a challenge to the security personnel to have an opportunity to make sure that these devices are safe and secure into and out of their network.

To confront these challenges, the following three standard approaches are suggested to help reduce information security risks:

a. A proactive, deep-defense approach
b. User training
c. Higher ed collaboration among institutions

2.8. Governance over Data Security

When Institutions of higher learning are not centralized, it's more challenging to govern data security and offer comprehensive cyber security. But still, decentralization has been the way in recent years. This therefore presents a complicated challenge to the institutions in ensuring comprehensive cyber security.

Cyber Security in Institutions of Higher Learning

Cyberspace has more involved to it than just the Internet and information and communications technologies. It is a field comparable to the fields of land, air, sea, and space, but then again with its own distinct physiognomies and challenges. The cyber domain is characterized by the digital storage, update, and exchange of data through networked schemes and supported by critical information technology infrastructures. According to the National Security Strategy (Ministry of Information, Communications and Technology, 2014), Cyberspace has both national and global dimensions that comprise of industry, business, intellectual property, security, technology, philosophy, policy, and international relations. As such, cyberspace plays a critical role in the global economy. In Kenya, the Kenya Information and Communications Act (2013) defines cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, actions, training, best practices that can be used to protect the cyber environment,".

To ensure that institutions of higher learning are able to protect how students, faculty and staff interact, collaborate, and conduct business in the cyberspace, there will be a necessity to provide comprehensive cyber security adopting a re-architect Security.

This is one of the few real solutions to make security a built-in feature of all computing elements. Yes, it's time to abandon the assumptions that computers are only used by well-intentioned professors, that the only treasured data stored on those computers is drafts of research papers, and that the only other users on the network are university colleagues (Jan, Ronald, & Dieter, 2011). Instead, there is a need to take several specific steps including:

i. Digitally sign all data to prevent interference and develop a way to notify users whether something is from a reliable source (David & Michael, 2013). This is to say, replace current senseless security notices that users don't understand because they expose the guts of the technology. For instance, statements such as, "The security certificate has expired or is not yet valid." May not make sense to a lay person
ii. **Encrypt** all data and information at all epochs, except when it's presented on the screen (Kai, Marcel, Bastian, & Markus, 2018). Particularly, do not transmit plaintext email or other information across the Internet (David, Robert, & Matthew, 2012). Anything leaving your computer should be encrypted.
iii. Ensure you turn all security settings on by default especially because most users don't mess with defaults (Eric, 2018). Then, make it easy to adjust settings so that users can get trusted activities performed without having to open a Pandora box for everybody.
iv. Ensure to automate virtually all updates. Most antivirus software downloads new virus definitions in the background. There is also automated patching such which are also an improvement.
v. **Polish** security features through heavy user testing and detailed field research are a must. This will always crop up any possible point of weakness to early attention.
vi. Implementing cyber security techniques such as access control and password security, authentication and authorization of data, malware scanners, firewalls, anti-virus software and data backups etc.
vii. There are **numerous other desired steps as well, including non-usability issues for example reducing the amount of software bugs.**

3. Methodology

3.1. Research design

In this paper, descriptive survey research design was implemented. Secondary data was reviewed from the Kenyan Ministry of planning and ICT authority's cyber security report of 2014 which was subjected to systematic literature review to draw meaning. This was mainly done because there was need to collect data from a sample that has been selected to characterize a population to which the findings of the data analysis could be generalised. This is

how survey design was considered appropriate for such studies.

3.2. Area of the study

This study was carried out on institutions of higher learning in Kenya and a sample of 35 institutions was considered. There was specific data mining on cyber security and security policies in those institutions.

3.3. Method of Data Collection

Secondary data was collected from institutions that already conducted a thorough research such as the Kenya Bureau of statistics and the Communication Authority of Kenya. Thanks to the open data policy adopted by the Kenyan government.

4. Results

According to the Public Sector ICT Survey Report (2016), learning institutions are highly affected by cyber-attacks as indicated in the graph below (Communications Authority of Kenya; Kenya National Bureau of Statistics, 2017).

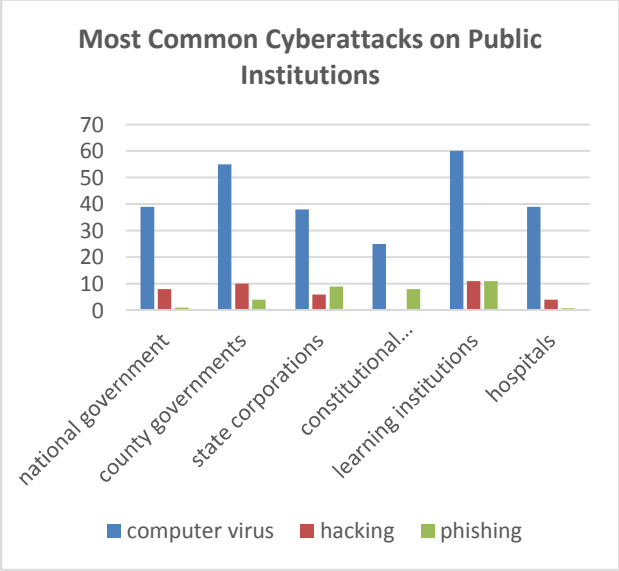

Figure 1: Public Sector ICT Survey Report 2016

5. Conclusion

Institutions of higher learning in Kenya and indeed in Africa and the globe in general are facing highly increasing cyber-threats. This inclination underscores the importance of reinforcing the responsible cyber security measures. This means that institutions of higher learning must upturn investment in cyber security technologies, provide cyber security-related training to staff and students and employ security professionals to run their cyber security space. It is also imperative to create cyber security awareness among all stakeholders.

Policy makers in higher education sector should increase public awareness of cyber security practices and consolidating regulatory policies and enforcement capabilities in the area of cyber security.

Finally, Institutions of higher learning must take a more proactive style to minimize and criminalize cybersecurity. Computer security is a huge theme that is becoming more significant because the globe is increasingly becoming extremely interconnected, with critical transactions being carried out on the internet. Cybercrime continues to deviate into different tracks with each new day that passes and so does the security or insecurity thereof of data and information bringing to rise other latest and disruptive technologies, along with the new cyber tools and threats. Therefore, institutions of higher learning must keep up the pace.

Recommendation

Out of this research, we recommend that institutions of higher learning should invest in up to date research laboratories and put more emphasis on research and development of cyber security within their institutions individually and collectively while at the same time emphasizing that the top management allocates appropriate financial resources to cyber security.

Another recommendation we make is that these should send their students and staff for exchange programs to other universities and industry especially to developed nations to learn best and applicable practices to mitigate cyber security relate d threats.

Equally, there is need for institutions of higher learning to organize frequent cyber security trainings and conferences for all staff and students and more especially to all those whose responsibility is in ensuring organizational cyber security including senior management.

We also recommend that institutions of higher learning train their students and staff on Cyber Ethics. Cyber ethics refers to the code of conduct on the internet. When students and staff of these institutions and indeed any other internet users exercise this basic code, there are decent probabilities of treating all users consuming the

internet in a proper and safer way (Lee, 2019). Here below are some of them according to (Nikhita & Ugander, 2014):

i. USE the Internet to connect and interrelate with other people wisely. Email and instant messaging (Social media) make it easy to stay in contact with friends and family, connect with workmates and share thoughts and information with people across different geographical locations.
ii. DON'T be an Internet bully. Do not abuse people or lie about them or send disconcerting pictures of them or do whatever else to try to hurt other people.
iii. Always acknowledge sources of your information. Internet is well-thought-out as the world's prime library with data and information on virtually any topic in any subject. So, use this data or information in an accurate and legal way.
iv. DO NOT operate others' accounts using their authentication.
v. NEVER send or try to send any kind of malware to other's systems or other people's computers to try and make corrupt them.
vi. NEVER share your individual information to just anybody because there is a possibility of other people abusing it and lastly you would end up in a distress.
vii. When online do not pretend to others and never create fake accounts on someone else. This would land you as well as the other person into misfortune.
viii. Always stick to copyrighted data or information and download material or games or videos only if they are permitted.

The above are a few cyber ethics that one should adhere to while using the internet. We are always thought proper rules from very early stages in life and right the same way here we are suggested with this basic code that we should all apply in our cyber space.

References

[1] Ashwin, P. (2016, August 10). Security is more than User Education – it's About Cultural Change. Retrieved from www.cso.com.au: https://www.cso.com.au/article/604844/security-more-than-user-education-it-about-cultural-change/

[2] Cheng, L. (2016). Chinese Politics in the Xi Jinping Era: Reassessing Collective Leadership. Washington, D.C.: Brookings Institution Press.

[3] Christopher, H., & Michele, F. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Hoboken, New Jersey: Wiley.

[4] Communications Authority of Kenya; Kenya National Bureau of Statistics. (2017). The Public Sector ICT survey 2016. Nairobi: Kenya National Bureau of Statistics.

[5] David, B. (2016, June 5th). 6 Common Phishing Attacks and How to Protect Against Them. Retrieved August 13, 2019, from The State of Security: https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

[6] David, D. L., Robert, A. K., & Matthew, C. M. (2012). mHealth Data Security: The Need for HIPAA-Compliant Standardization. Telemedicine and e-Health, 18(4), 284 - 288.

[7] David, H. (2017, August 29). Security and Education. Retrieved from welivesecurity.com: https://www.welivesecurity.com/2017/08/29/security-and-education/

[8] David, K., & Michael, G. S. (2013). Fundamentals of Information Systems Security. Burlington, Massachusetts: Jones & Bartlett Publishers.

[9] EDUCAUSE. (n.d.). Building Technology Strategy that Enables Next Generation Enterprise IT. Retrieved July 12, 2019, from www.educause.edu: https://www.educause.edu/focus-areas-and-initiatives/enterprise-and-infrastructure/enterprise-it-program/building-technology-strategy-that-enables-next-generation-enterprise-it

[10] Eric, B. (2018). Using Security Apps and Backup. Berkeley, CA: Apress,.

[11] Folashade, B. O., & Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), 98 - 114.

[12] Harold, F. T., & Micki, K. (2003). Information Security Management Handbook. Boca Raton, Florida: CRC Press.

[13] Jakob, N. (2004, October 25). User Education Is Not the Answer to Security Problems. Retrieved from Nielsen Norman Group: World Leaders in Research-Based User Experience: https://www.nngroup.com/articles/security-and-user-education/

[14] Jan, C., Ronald, L., & Dieter, S. (2011). Digital Privacy: PRIME - Privacy and Identity Management for Europe. Heidelberg, Germany: Springer Science & Business Media.

[15] Kai, G., Marcel, T., Bastian, W., & Markus, R. (2018). Comparison of approaches to encrypt data for supply chain simulation applications in cloud environments. WSC '18 Proceedings of the 2018 Winter Simulation Conference. Gothenburg, Sweden: IEEE Press Piscataway, NJ, USA.

[16] Lee, Y.-J. (2019). Masese Bogomba Nelson holds PhD from Kibabii University Kenya, He is currently. IndianJournals.com, 19(2).

[17] Ministry of Information, Communications and Technology. (2014, April 20). National Security Strategy 2014. Nairobi. Retrieved August 2019, 13th, from

http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf

[18] Mostafa, E., Mohamed, B., & Faddoul, K. (2017). Advanced Information Technology, Services and Systems: Proceedings of the International Conference on Advanced Information Technology, Services and Systems (AIT2S-17) Held on April 14/15, 2017 in Tangier. York City: Springer.

[19] Nikhita, R. G., & Ugander, R. G. (2014, January). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. International Journal of Engineering and Technology, Volume 4 (1).

[20] Peter, M., & Kenneth, E. (2018). Design and Analysis for Quantitative Research in Music Education. Oxford, U.K: Oxford University Press.

[21] Resources Management, A. I. (Ed.). (2018). Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications. Hershey, Pennsylvania: IGI Global.

[22] Tanya, R. (2015, November 2). The Top 10 Higher Ed IT Issues of 2016. Retrieved August 13, 2019, from Center for Digital Education (EDUCAUSE): https://www.govtech.com/education/higher-ed/The-Top-10-Higher-Ed-IT-Issues-of-2016.html

[23] Tanya, R. (2016, May 18). 8 Cybersecurity Challenges Facing Higher Education. Retrieved August 13, 2019, from Centre for Digital Education: https://www.govtech.com/education/higher-ed/8-Cybersecurity-Challenges-Facing-Higher-Education.html

[24] Trend, M. (2015, March 9). The challenges of cyber security education and training in 2015. Retrieved from https://blog.trendmicro.com: https://blog.trendmicro.com/the-challenges-of-cyber-security-education-and-training-in-2015/

Authors –

Mayieka Jared Maranga is a PhD student at Kabarak University-Kenya. He holds a Master of Science in Information Technology degree [2012] and Bachelor of Business Information Technology [2009] from Strathmore University; He has worked as: a graduate assistant at Strathmore University (2009 - 2012), an assistant lecturer at Strathmore University's Faculty of Information Technology (2012 – 2014), adjunct faculty as United States International University's School of Science and Technology (2015 - 2016) and an assistant lecturer at Africa International University (2016 to date). His current research interests are generally around Computer Security and Audit and Databases.

Masese Bogomba Nelson holds PhD from Kibabii University Kenya. He is currently a lecturer in Information Technology at Kabarak University Kenya. His research interests include mobile applications, security and IoT.